国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 02 月 03 日-2020 年 02 月 09 日　　2020 年第 6 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 573 个，其中高危漏洞 211 个、中危漏洞 317 个、低危漏洞 45 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 178 个（占 31%），其中互联网上出现“WordPress Core xmlrpc.php 拒绝服务漏洞、TP-Link Archer VR300 跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1729 个，与上周（933 个）环比增加 85%。

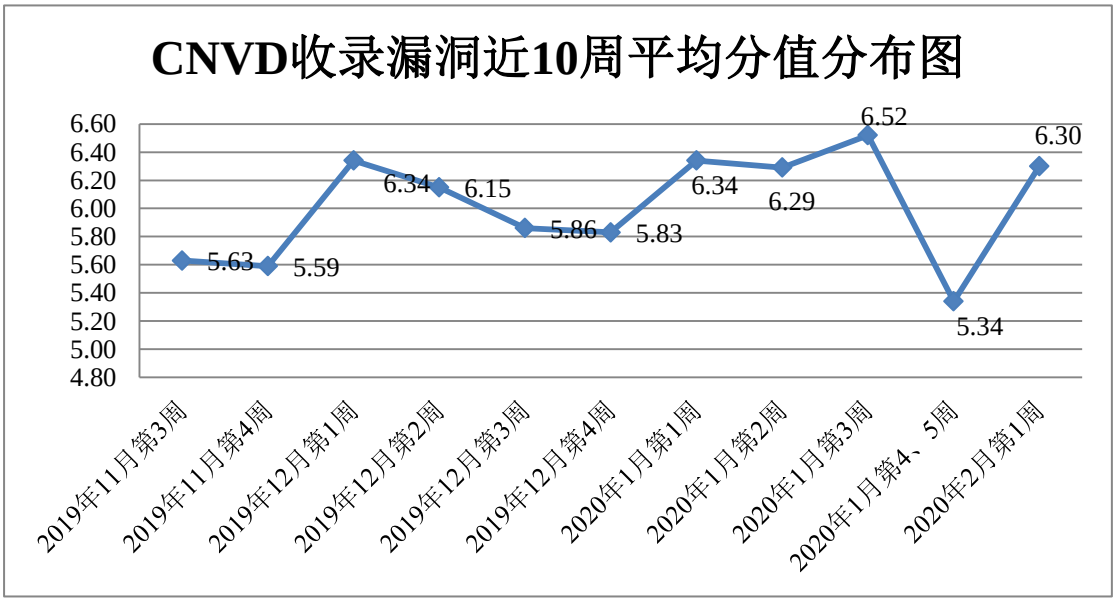

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 14 起，向基础电信企业通报漏洞事件 9 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞

事件 222 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 12 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 16 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

长城宽带网络服务有限公司、淄博闪灵网络科技有限公司、长沙德尚网络科技有限公司、北京金山安全管理系统技术有限公司、浙江贰贰网络有限公司、天津恩众科技发展有限公司、新天科技股份有限公司、友讯电子设备（上海）有限公司、上海亿速网络科技有限公司、成都市智蜂网科技有限责任公司、台湾永宏电机股份有限公司、施耐德电气有限公司、南昌卓蓝科技有限公司、深圳市科皓信息技术有限公司、南京南软科技有限公司、北京良精志诚科技有限责任公司、成都智蜂网科技有限责任公司、北京椒图科技有限公司、威锋国际公司、成都鹏博士电信传媒集团股份有限公司、成都爱米秀科技有限责任公司、湖南心艾网络科技有限公司、中国船舶集团有限公司、上海创旗天下科技股份有限公司、广州本盈计算机科技有限公司、青岛自动化仪表有限公司、秦皇岛商景科技有限公司、科擎科技有限公司、中粮集团有限公司、金山软件股份有限公司、苏州卡达网络科技有限公司、万商云集(成都)科技股份有限公司、华科企业管理系统、国家卫生健康委国际交流与合作中心、帝国软件、新秀工作室、海洋 CMS、MoMoCMS、AKCMS、ZhiCms、Wordpress、Catfish CMS、NetSarang 和 UQCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。内蒙古洞明科技有限公司、北京华云安信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、河南灵创电子科技有限公司、长春嘉诚信息技术股份有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、北京圣博润高新技术股份有限公司、北京小米科技有限责任公司、南京森林警察学院网络安全工作室及其他个人白帽子向 CNVD 提交了 1729 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 1089 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
斗象科技（漏洞盒子）	607	607

北京天融信网络安全技术有限公司	273	6
奇安信网神（补天平台）	257	257
上海交大	225	225
北京启明星辰信息安全技术有限公司	129	0
恒安嘉新(北京)科技股份公司	36	0
哈尔滨安天科技集团股份有限公司	31	0
北京神州绿盟科技有限公司	26	0
华为技术有限公司	23	0
北京知道创宇信息技术股份有限公司	3	0
内蒙古洞明科技有限公司	160	160
北京华云安信息技术有限公司	57	57
远江盛邦（北京）网络安全科技股份有限公司	44	44
河南灵创电子科技有限公司	43	43
长春嘉诚信息技术股份有限公司	41	41
国瑞数码零点实验室	10	10
内蒙古奥创科技有限公司	8	8
北京圣博润高新技术股份有限公司	4	4
北京小米科技有限责任公司	2	2
南京森林警察学院网络安全工作室	1	1
CNCERT 海南分中心	1	1
个人	263	263
报送总计	2244	1729

本周漏洞按类型和厂商统计

本周，CNVD 收录了 573 个漏洞。应用程序 376 个，WEB 应用 105 个，操作系统 34 个，网络设备（交换机、路由器等网络端设备）29 个，安全产品 19 个，数据库 5 个，智能设备（物联网终端设备）5 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序	376
WEB 应用	105
操作系统	34
网络设备（交换机、路由器等网络端设备）	29
安全产品	19
数据库	5
智能设备（物联网终端设备）漏洞	5

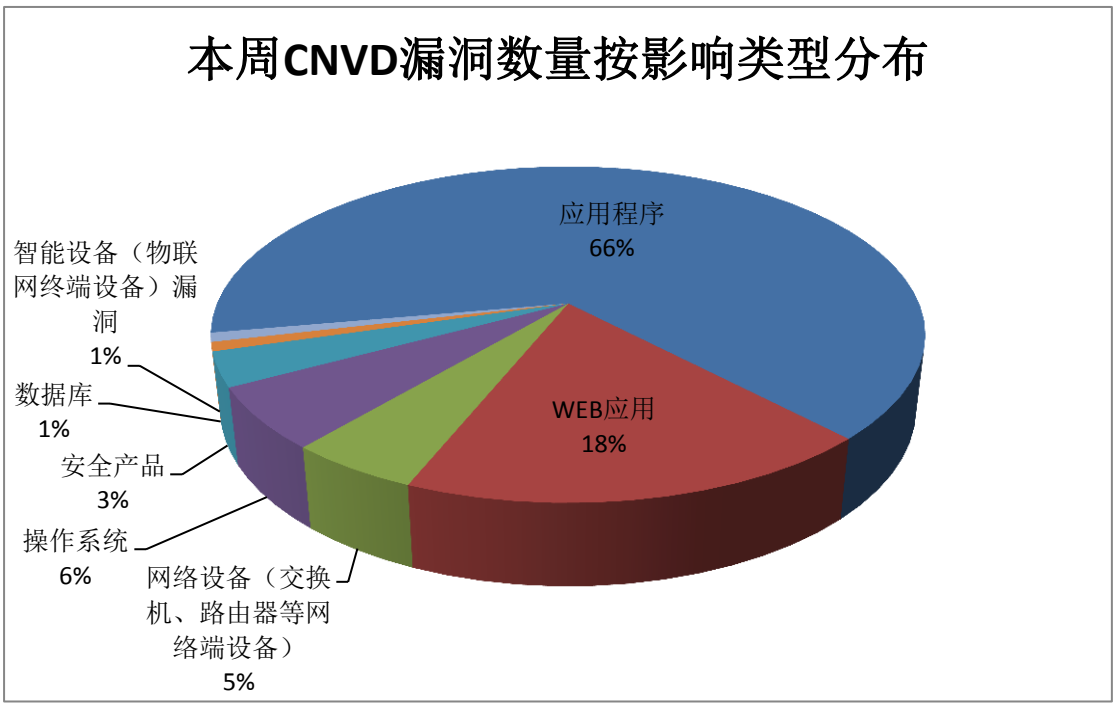

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Cisco、GitLab 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	81	14%
2	Cisco	23	4%
3	GitLab	20	4%

4	Adobe	16	3%
5	Microsoft	15	3%
6	cPanel	14	2%
7	GNU	14	2%
8	WordPress	13	2%
9	Apple	12	2%
10	其他	365	64%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，17 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Cisco IOS 和 Cisco IOS XE Software 跨站请求伪造漏洞、Microsoft .NET Framework 远程代码执行漏洞（CNVD-2020-03547）、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-03858）、WAGO PFC 200 ‘I/O-Check’缓冲区溢出漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

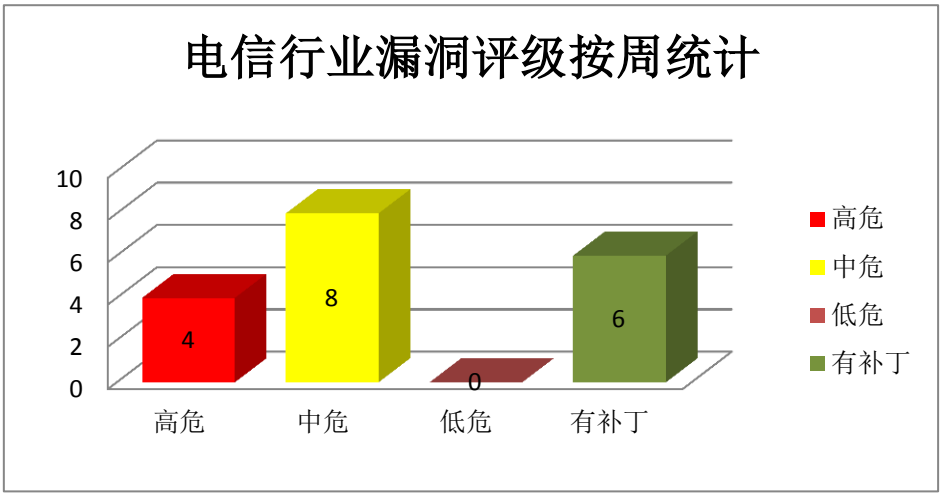

图 3 电信行业漏洞统计

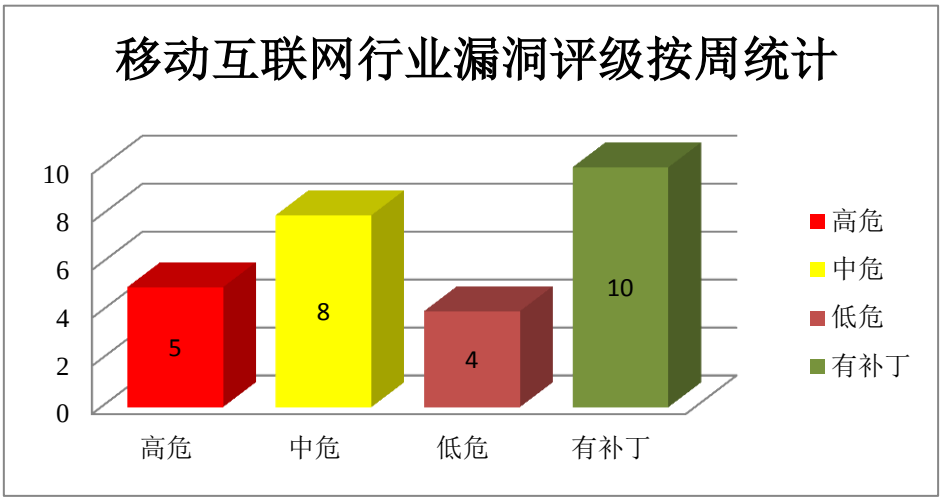

图 4 移动互联网行业漏洞统计

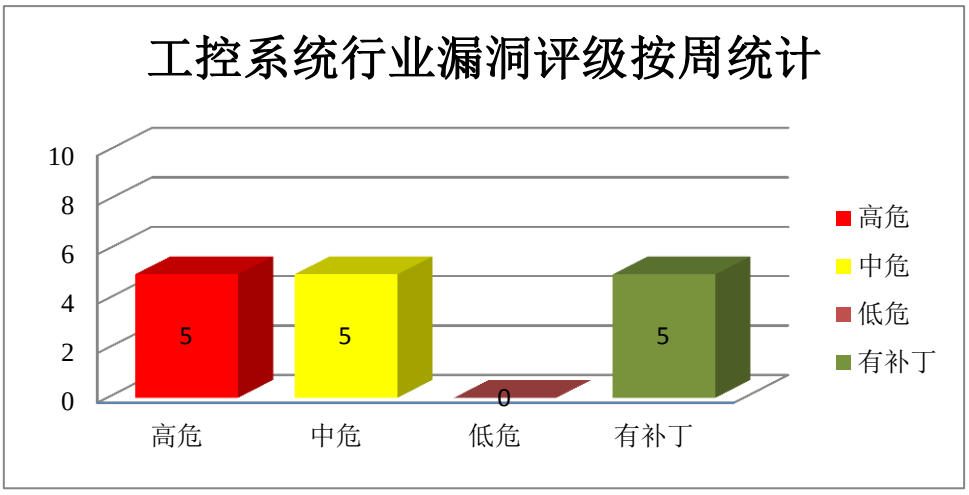

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Apple 产品安全漏洞

Apple macOS Catalina 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。Apple iOS 是一款苹果智能设备上的操作系统。Apple macOS Mojave 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。Apple tvOS 是一套智能电视操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行代码，提升权限。

CNVD 收录的相关漏洞包括：Apple macOS AppleGraphicsControl 组件内存破坏漏洞、Apple macOS Catalina System Extensions 组件权限提升漏洞、Apple macOS Catalina、tvOS 和 iOS libxml2 组件存在内存破坏漏洞、Apple macOS Catalina 的 Intel Graphics Driver 组件内存损坏漏洞、Apple macOS 任意代码执行漏洞（CNVD-2020-03281）、

Apple iOS AppleFirmwareUpdateKext 任意代码执行漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-03858）、多款 Apple 产品 IOUSBDeviceFamily 组件内存破坏漏洞。其中，“Apple iOS AppleFirmwareUpdateKext 任意代码执行漏洞、Apple mac OS Catalina 的 Intel Graphics Driver 组件内存损坏漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-03858）、多款 Apple 产品 IOUSBDeviceFamily 组件内存破坏漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03276
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03282
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03283
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03280
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03281
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03284
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03858
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03862

2、Microsoft 产品安全漏洞

Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Microsoft .NET Framework 是美国微软（Microsoft）公司的一种全面且一致的编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，提升权限，控制受影响的系统。

CNVD 收录的相关漏洞包括：Microsoft Excel 远程代码执行漏洞（CNVD-2020-03534、CNVD-2020-03536）、Microsoft Office 远程代码执行漏洞（CNVD-2020-03535）、Microsoft Excel 代码执行漏洞、Microsoft Windows 和 Microsoft Windows Server 提权漏洞（CNVD-2020-03545、CNVD-2020-03546、CNVD-2020-03548）、Microsoft .NET Framework 远程代码执行漏洞（CNVD-2020-03547）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03534
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03535
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03536
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03537
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03545

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03546

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03547

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03548

3、Cisco 产品安全漏洞

Cisco IOS 和 IOS XE Software 都是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco Webex Video Mesh Software releases 是一款网络视频会议解决方案。Cisco Hosted Collaboration Mediation Fulfillment (HCM-F)是托管式协作解决方案(HCS)的一部分，是一个核心管理组件。Cisco SD-WAN Solution 是一套网络扩展解决方案，vManage 是其中的控制台。Cisco IOS XR 软件是用于服务提供商网络的模块化和完全分布式的网络操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞修改配置和数据库表中的条目，执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco IOS 和 Cisco IOS XE Software 跨站请求伪造漏洞、Cisco Webex Video Mesh Software 命令注入漏洞 、Cisco Hosted Collaboration Mediation Fulfillment 跨站请求伪造漏洞（CNVD-2020-03756）、Cisco IOS XR BGP 属性拒绝服务漏洞、Cisco SD-WAN Solution SQL 注入漏洞（CNVD-2020-04036、CNVD-2020-03759）、Cisco IOS XR BGP EVPN 拒绝服务漏洞（CNVD-2020-04037）、Cisco IOS XR 拒绝服务漏洞（CNVD-2020-04053）。其中，“Cisco IOS 和 Cisco IOS XE Software 跨站请求伪造漏洞、Cisco Webex Video Mesh Software 命令注入漏洞 、Cisco Hosted Collaboration Mediation Fulfillment 跨站请求伪造漏洞（CNVD-2020-03756）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03723

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03752

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03756

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03759

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03762

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04036

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04037

http://www.cnvd.org.cn/flaw/show/CNVD-2020-04053

4、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品。前者是一套 PDF 文件编辑和转换工具，后者是一套 PDF 文档阅读软件。Illustrator CC 是一款矢量图制作工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，获取敏感信息访问权限，导致拒绝服务。

CNVD 收录的相关漏洞包括：Adobe Illustrator CC 内存损坏漏洞（CNVD-2020-03

924、CNVD-2020-03923）、Adobe Acrobat 和 Reader 存在堆缓冲区溢出漏洞（CNVD-2020-04323）、Adobe Acrobat 和 Reader 存在内存越界读取漏洞（CNVD-2020-04322、CNVD-2020-04324、CNVD-2020-04325、CNVD-2020-04328、CNVD-2020-04331）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03923
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03924
http://www.cnvd.org.cn/flaw/show/CNVD-2020-04323
http://www.cnvd.org.cn/flaw/show/CNVD-2020-04322
http://www.cnvd.org.cn/flaw/show/CNVD-2020-04324
http://www.cnvd.org.cn/flaw/show/CNVD-2020-04325
http://www.cnvd.org.cn/flaw/show/CNVD-2020-04328
http://www.cnvd.org.cn/flaw/show/CNVD-2020-04331

5、Apache XML-RPC 代码问题漏洞

Apache XML-RPC 是美国阿帕奇（Apache）软件基金会的一款 XML-RPC（远程过程调用协议）的 Java 实现。本周，Apache XML-RPC 被披露存在代码问题漏洞。攻击者可利用该漏洞获取网址敏感信息。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03927

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2020-03250	Facebook WhatsApp 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.facebook.com/security/advisories/cve-2019-18426
CNVD-2020-03563	GNU LibreDWG 双重释放漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/LibreDWG/libredwg/compare/0.9.2...0.9.3
CNVD-2020-03580	多款 Qualcomm 产品缓冲区溢出漏洞（CNVD-2020-03580）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin
CNVD-202	PHP 内存位置双重释放漏洞	高	目前厂商已发布升级补丁以修复漏

0-03582			洞，补丁获取链接：https://bugs.php.net/bug.php?id=78943
CNVD-2020-03585	IBM Cognos Business Intelligence 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ibm.com/support/pages/node/1142626
CNVD-2020-03748	Atlassian Crowd 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.atlassian.com/browse/CWD-5091
CNVD-2020-03860	Dell XPS 13 2-in-1 BIOS 配置错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/article/SLN319808
CNVD-2020-03900	DLINKDIR-859 系列路由器存在命令执行漏洞	高	厂商已修复该漏洞，请关注厂商主页更新：https://www.dlink.com
CNVD-2020-03937	Huawei GaussDB 200 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20200120-01-gaussdb200-cn
CNVD-2020-04138	Micro Focus ArcSight Logger 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://community.microfocus.com/t5/Logger/Logger-Release-Notes-7-0/ta-p/2750305

小结：本周，Apple 产品被披露存在多个漏洞，攻击者可利用漏洞执行代码，提升权限。此外，Microsoft、Cisco、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，提升权限，导致拒绝服务等。另外，Apache XML-RPC 被披露存在代码问题漏洞。攻击者可利用该漏洞获取网址敏感信息。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、TP-Link Archer VR300 跨站脚本漏洞

验证描述

TP-Link Archer VR300 是中国普联（TP-Link）公司的一款调制解调器路由器。

TP-Link Archer VR300 存在跨站脚本漏洞，攻击者可利用该漏洞获取 Cookie 或重

定向到恶意网站。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2019110101

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-03765

信息提供者

CNVD 工作组

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Windows 7 bug 阻止用户关机或重启

Windows 7用户报告一个未知原因的bug会导致在尝试关机或重启时弹出警告信息“你没有权限关闭这台计算机”。Windows 7 已在今年 1 月结束支持，意味着微软不再可能会向 Windows 7 系统释出补丁。不过微软表示它会修复 Windows 7 最后一批补丁引入的黑屏幕 bug。对于最新的阻止关机 bug，目前还不清楚微软是否会修。

参考链接：https://www.solidot.org/story?sid=63461

2. 思科大量设备中招：思科发现协议的高危漏洞

物联网网络安全网络 Armis 在实施思科发现协议（CDP）的各种设备中发现了五个危急的零日漏洞，这些漏洞使远程攻击者无需任何用户干预就可以全面接管设备。CDP 是思科的一种专有第 2 层（数据链路层）网络协议，用于发现有关本地连接的思科设备的信息。

参考链接：https://nosec.org/home/detail/4082.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等

工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537